REMARKS

Claims 8, 11, 25, and 27 are amended. Claims 1-41 remain in the Application. Reconsideration of the pending claims is respectfully requested in view of the above amendments and the following remarks.

I. Claims Rejected Under 35 U.S.C. § 112

Claims 8 and 11 stand rejected under 35 U.S.C. § 112, because "the first password P_B" has insufficient antecedent basis. Applicants amend Claims 8 and 11 to replace "the first password P_B" with "a first password P_B."

Although not identified by the Examiner, Applicants also amend Claims 25 and 27 to recite "a first password P_B" for the same reason mentioned above in regard to Claims 8 and 11. Claim 27 is further amended to recite "the first secret S_B" which has a proper antecedent basis in claim 24.

Accordingly, reconsideration and withdrawal of the § 112 rejection of Claims 8 and 11 are respectfully requested.

II. Claims Rejected Under 35 U.S.C. § 103

A. Claims 1-5, 12, 13, 17-22, 24, 26, and 34-40 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,953,424 issued to Vogelesang et al. ("Vogelesang"), in view of Menezes, Alfred J., Handbook of Applied Crytography, CRC Press, 1997, pages 234-237 ("Menezes"). Applicants respectfully traverse the rejection.

To establish a *prima facie* case of obviousness, the relied upon references must teach or suggest every limitation of the claim such that the invention as a whole would have been obvious at the time the invention was made to one skilled in the art.

Claim 1 recites the elements of "generating, at the first entity, a first session key K_B and a first secret S_B, the first session key K_B being different from the first secret S_B, **both the first session key K_B and the first secret S_B being computed from the second public key M_A**" (emphasis added). Applicants submit that Vogelesang in view of Menezes does not teach or suggest at least these elements.

Vogelesang discloses a cryptographic system in which signals between two participants are encrypted with one encryption key (i.e., a shared secret S). The Examiner recognizes that Vogelesang does not disclose encryption with two encryption keys, but relies on Menezes to cure this deficiency.

Menezes discloses encrypting a message with two encryption keys. Menezes discloses that the two encryption keys are independent of each other (see definition 7.29 of Menezes). However, Menezes does not disclose using two different encryption keys, both of which are computed from the same public key. As the two encryption keys of Menezes are independent of each other, they cannot be dependent on the same public key. Thus, the two encryption keys of Menezes cannot be computed from the same public key. Thus, Vogelesang is view of Menezes does not teach or suggest the first session key K_B and the first secret S_B that are computed from the same public key.

Claims 2-5, 12, 13, and 17-19 depend from Claim 1 and incorporate the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claim 1, these claims are non-obvious over Vogelesang and Menezes. Analogous discussions apply to independent Claims 20-22, 24, and 38-40. Claims 26 and 34-37 depend from Claim 24 and incorporate the limitations thereof. Thus, for at least the reasons mentioned above, these claims are non-obvious over Vogelesang and Menezes.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claims 1-5, 12, 13, 17-22, 24, 26, and 34-40 are respectfully requested.

B. Claims 6-9, 11, and 27-32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Vogelesang in view of Menezes in further view of Wu, Thomas, "The Secure Remote Password Protocol," November 11, 1997, Stanford University, pages 1-17 ("Wu").

Claims 6-9, 11, and 27-32 depend from Claims 1 and 24, respectively, and incorporate the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claims 1 and 24, Vogelesang and Menezes do not teach or suggest each of the elements of these claims.

Wu does not cure the deficiencies of Vogelesang and Menezes. Wu discloses a password authentication and key exchange protocol (see, e.g., Abstract). However, the Examiner has not identified and Applicants have been unable to discern any part of Wu that discloses encrypting a message using two different keys that are computed from the same public key. Thus, the cited references, separately or combined, do not teach or suggest each of the elements of Claims 6-9, 11, and 27-32.

Moreover, with respect to Claims 6 and 27, Wu does not disclose that "the first secret S_B is generated using a combining function f_B on at least a first password P_B and the first public key M_B." Wu does not disclose using the combining function f to generate a secret. Rather, Wu discloses that the result (B) generated by the combining function f is sent to another party in the open (i.e., in an unencrypted form). An openly transmitted message cannot be a secret. Thus, Wu does not disclose generating a secret using the combining function as claimed. Thus, the cited references do not teach or suggest Claims 6 and 27 for this additional reason.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claims 6-9, 11, and 27-32 are respectfully requested.

C. Claims 10 and 31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Vogelesang in view of Menezes, and further in view of Wu.

Claims 10 and 31 depend from Claims 1 and 24, respectively, and incorporate the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claims 1 and 24, Vogelesang and Menezes do not teach or suggest each element of these claims.

Wu does not cure the deficiencies of Vogelesang and Menezes. The Examiner has not identified and Applicants have been unable to discern any part of Wu that discloses encrypting a message using two different keys that are computed from the same public key. Thus, the cited references, separately or combined, do not teach or suggest each of the elements of Claims 10 and 31.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claims 10 and 31 are respectfully requested.

D. Claims 14-16, 25, and 33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Vogelesang in view of Menezes.

Claims 14-16, 25, and 33 depend from Claims 1 and 24, respectively, and incorporate the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claims 1 and 24, Vogelesang in view of Menezes does not teach or suggest each of the elements of these dependent claims.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claims 14-16, 25 and 33 are requested.

E. Claim 41 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Vogelesang in view of Menezes.

Claim 41 depends from Claim 40 and incorporates the limitations thereof. Claim 40 is non-obvious over Vogelesang in view of Menezes for reasons analogous to Claim 1. Thus, for at least the reasons mentioned above in regard to Claim 1, Vogelesang in view of Menezes does not teach or suggest each of the elements of Claim 40.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claim 40 are requested.

F. Claim 23 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Vogelesang in view of Menezes.

The omission of Claim 23 in the previous response was caused by a clerical error and is therefore not an indication of acquiescence to the rejection.

Claim 23 depends from Claim 1 and incorporates the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claim 1, Vogelesang in view of Menezes does not teach or suggest each of the elements of Claim 23.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claim 23 are requested.

CONCLUSION

In view of the foregoing, it is believed that all claims are now in condition for allowance and such action is earnestly solicited at the earliest possible date. If there are any additional fees due in connection with the filing of this response, please charge those fees to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: October 2, 2006

Jonathan S. Miller, Reg. No. 48,534

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF MAILING:
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Amber D Saunders 10/2/06

Amber D. Saunders Date